

Claims

1. A system for protecting information received over a network comprising:
at least one first computer system connected to said network;
a plurality of second computer systems capable of connecting to said first computer system through said network in which each of said second computers has a user interface to enable the user of the second computer to interact with the second computer system;
means for registering at said first computer system one or more of said second computer systems with said first computer system;
means for sending content information from the first computer system to at least one of said registered second computer systems without associated information defining the use of said content information by said second computer systems; and
means for enabling display of the received content information at the registered second computer system which receives the content information and limiting the user interface of the second computer system to operate responsive to the user of the second computer system to prevent copying of the content information when said received content information is being displayed.
2. The system according to Claim 1 wherein said content information sent to said one of said registered second computer systems is encrypted, further comprising:
means at said second computer system for requesting a key from said first computer system for decrypting said received encrypted content information;
means at said first computer system for sending a key to decrypt the encrypted content information to the second computer system which requested the key; and
means at the second computer system for decrypting the encrypted content information in accordance with the received key, in which said second computer system when displaying the decrypted content information ignores signals from the user interface capable of enabling access to the decrypted content information.
3. The system according to Claim 2 wherein one or more of said registered second computer systems are preselected to view the content information, and said key sending means only sends said key to said preselected second computer systems.

4. The system according to Claim 2 wherein said key sending means only sends said key during a certain time period.

5. The system according to Claim 2 wherein said key sending means only send said key to said second computer system a certain number of times.

6. The system according to Claim 1 wherein said display enabling means at said second computer systems is provided by viewer software installed at the second computer system, and said registering means is enabled when said viewer software is installed.

7. The system according to Claim 1 wherein said sending means, and display enabling means are enabled by viewer software installed at the second computer system.

8. The system according to Claim 7 wherein said viewer software is automatically executed in response to executing a program received by said second computer system via the network.

9. The system according to Claim 1 wherein said second computer systems have a display, and said display enabling means provides for playing said content information is a window on the display.

10. The system according to Claim 9 wherein said display enabling means disables playing of said content information in said window when the user of the second computer system selects another window on the display.

11. The system according to Claim 10 wherein said display enabling means places a protection image in the window when said playing of said content information in said window is disabled.

12. The system according to Claim 1 wherein said first computer system comprises one or more server computers and a database coupled to at least one of said server computers containing at least information defining the registered second computers.

13. The system according to Claim 1 wherein said second computer systems each have means for interfacing to said network and capable of connecting to said first computer system at one or more network addresses.

14. The system according to Claim 1 wherein said network represents a public network.

15. The system according to Claim 1 wherein said content information is part of a survey.

16. The system according to Claim 15 wherein said first computer system comprises one or more server computers capable of communicating with said plurality of second computer systems via said network, and a database coupled to at least one of said network computers containing at least information defining the registered second computer systems, information identifying which of the registered ones of said second computer systems are associated with participants for the survey, and information determining whether the survey was taken by the participants, in which said content information is sent encrypted by said first computer system, said first computer system has means for sending to said second computer systems a key to decrypt the encrypted file when, in accordance with said database, said second computer system is associated with one of the participants for the survey not having taken the survey, and said second computer system has means for decrypting said encrypted content information in accordance with said key for displaying the decrypted content information.

17. A method for protecting information received over a network, such as the Internet, comprising the steps of:
providing at least one first computer system;

providing a plurality of second computer systems capable of connecting to said first computer system through said network in which each of said second computers has a user interface to enable the user of the second computer to interact with the second computer system;

registering at said first computer system one or more of said second computer systems with said first computer system;

sending content information from the first computer system to at least one of said registered second computer systems without associated information defining the use of said content information by said second computer systems; and

displaying of the received content information at the registered second computer system which receives the content information and limiting the user interface of the second computer system to operate responsive to the user of the second computer system to prevent copying of the content information when said received content information is being displayed.

18. The method according to Claim 17 wherein said content information sent to said one of said registered second computer systems is encrypted, said method further comprising the steps of:

requesting at said second computer system a key from said first computer system for decrypting said received encrypted content information;

sending from said first computer system a key to decrypt the encrypted content information to the second computer system which requested the key; and

decrypting at the second computer system the encrypted content information in accordance with the received key, in which said second computer system when displaying the decrypted content information ignores signals from the user interface capable of enabling access to the decrypted content information.

19. The method according to Claim 18 further comprising the step of selecting one or more of said registered second computer systems to display the content information, and said key sending step only sends said key to the preselected second computer systems which requested the key.

20. A method for conducting a survey at a computer connected to the Internet comprising the steps of:

sending a survey to the computer via the Internet which references a network address to obtain a file for said survey;

downloading said file from said network address in which said file is encrypted;

requesting a key to decrypt said encrypted file from a network address where said key is available;

receiving a key at the computer when said computer is associated with a participant selected to take said survey; and

decrypting the file in accordance with said key and playing the decrypted file as part of the survey.

21. The method according to Claim 20 further comprising the steps of:

playing the decrypted file in a window on a display coupled to the computer; and

protecting said window from being accessed by the user of the computer when another window on the display is selected.

22. The method according to Claim 20 further comprising the step of registering the computer for receiving said survey prior to carrying out said sending survey step.

23. The method according to Claim 20 wherein said receiving a key step further comprises the step of sending the key to the computer when said key has been requested during a certain period of time.

24. The method according to Claim 20 wherein said receiving a key step further comprises the step of sending the key to the computer when computer has not already received the encrypted file a preset number of times.

25. The method according to Claim 20 wherein said receiving a key step further comprises the step of sending the key to the computer when a participant has not taken the survey.

26. A system for protecting an information file received over a public network from a World Wide Web site by one or more computer systems capable of communicating via the network to the web site, said system comprising:

a web site connected to the network which uniquely registers one or more of said computer systems identifying said computer system to said web site and stores in a database encrypted information files and their associated keys, in which said web site is capable of sending said encrypted information file to registered computer systems, and sending a key to decrypt an encrypted information file to one of said registered second computer system when said second computer system is authorized to receive the key;

each of said computer system being capable of connecting to said web site through the Internet and registered with said web site to send a request to said web site for a certain encrypted information file and to receive the encrypted information file, and then request a key from said web site to decrypt the file, and in response to receiving the key, decrypts the encrypted information file and plays the file through a window on the display of the computer system; and

each of said computer systems having a display and a user interface in which, when said file is played, signals from the user interface at the second computer system are ignored which enable access to the decrypted file, and when another window is selected than the window displaying the decrypted file, disables the playing of the decrypted file.

27. An Internet web site for supporting concept surveys which are capable of connecting to one or more client computer systems comprising:

one or more computer servers capable of connecting to the Internet in which said client computer system are registered with said web site; and

a database coupled to one or more of said servers which stores encrypted information files representing parts of one or more surveys and their associated keys, in which said web site is capable of sending said encrypted information file to registered client computer systems for carrying out a survey received by said client computer systems, and sending a key to decrypt an encrypted information file to one of said registered second computer system when said second

computer system is authorized to receive the key to enable the client computer system to play the information file as part of the survey.

28. A system for protecting over the Internet viewed information received by one of a plurality of computer systems as part of a survey, said system comprising:

a web site connectable to each of the computer system in which said web site has a database storing encrypted content information and keys to decrypt the content information;

means for providing to each of the computer system from the web site a first identifier associated with a viewer;

means for registering each of the computer systems with the web site based on the first identifier provided from the web site and a second identifier uniquely identifying the computer system and storing in said database said first identifier in association with said second identifier;

means for inviting participants to take the survey associated with a unique third identifier in which said participants represent one or more of the registered computer systems;

means for providing to one of the computer system a file containing encrypted content information having a unique fourth identifier;

means at each of the computer system for receiving the survey and receiving the encrypted content information from the web site associated with the survey;

means at each of the computer systems for the viewer at the computer system for sending a request to the web site for a key to decrypt the encrypted content information in which said request has at least said first, second, third, and fourth identifiers;

means for the web site for sending a key to decrypt the encrypted content information file in accordance with the first, second, third, and fourth identifiers of the request matching corresponding identifiers associated with the participants invited to take the survey and exposure limit information associated with the encrypted content information;

means at each of the computer systems including the viewer for receiving the key from the web site, decrypting the encrypted content information based on the key, and opening a window on a display of the computer system to view the decrypted content information file; and

means at each of the computer systems for ignoring interrupts from user interface devices associated with the computer system which enable a user at the computer system to copy the

[illegible]